

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-101568

(43)Date of publication of application : 07.04.2000

(51)Int.Cl.

H04L 9/32
G06F 12/14
G06F 15/00
G11B 20/10

(21)Application number : 10-265211

(71)Applicant : FUJITSU LTD

(22)Date of filing : 18.09.1998

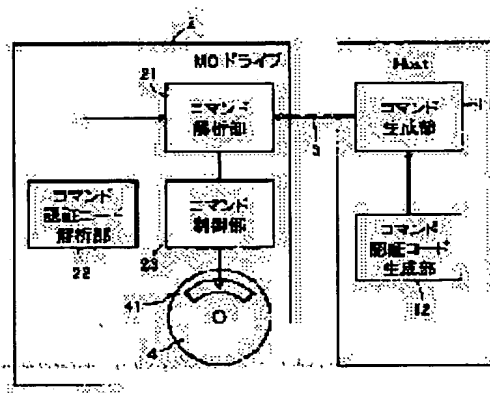
(72)Inventor : HIRANO HIDEYUKI
HASEBE TAKAYUKI
KOTANI MASATAKE

(54) COMMAND AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a command authentication method for preventing a command issued from a third person from setting itself up as the command by a normal user and maintaining high security.

SOLUTION: An authentication code in the command transmitted from a host 1 is collated by a command authentication code analysis part 22, and in the case of matching with information for collation, a specified command is generated by a command analysis part 21 and executed by a command control part 23. The specified command is executed based on authentication information in the command, it is difficult to analyze the authentication information and the high security is maintained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J.P.) (12) 公開特許公報 (A) (11) 特許出願公開番号

特開2000-101568

(P2000-101568A)

(43) 公開日 平成12年4月7日 (2000.4.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 C 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 C 5 D 0 4 4
G 1 1 B 20/10		G 1 1 B 20/10	D 5 J 1 0 4
		H 0 4 L 9/00	6 7 3 A
審査請求 未請求 請求項の数11 O L (全 6 頁)			

(21) 出願番号 特願平10-265211

(22) 出願日 平成10年9月18日 (1998.9.18)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 平野 秀幸

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 長谷部 高行

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100094145

弁理士 小野 由己男 (外2名)

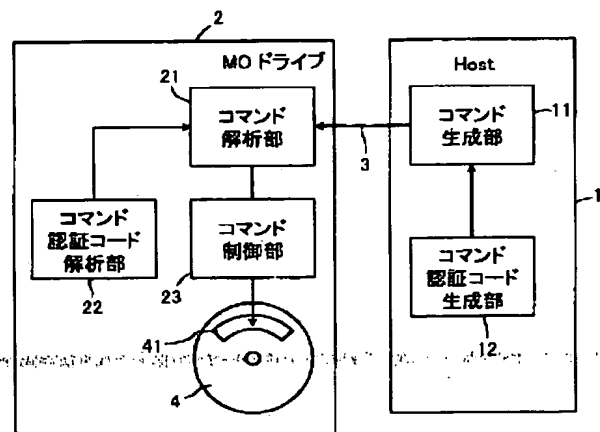
最終頁に続く

(54) 【発明の名称】 コマンド認証方法

(57) 【要約】

【課題】 第3者から発行されたコマンドが正規のユーザによるコマンドになりすますことを防止し、高いセキュリティを維持するコマンド認証方法を提案する。

【解決手段】 ホスト1から送信されてきたコマンド中の認証コードをコマンド認証コード解析部22によって照合し、照合用情報と合致した場合にはコマンド解析部21によって特定のコマンドを生成してコマンド制御部23に実行させる。



【特許請求の範囲】

【請求項1】受信したコマンドから認証情報を抽出し、前記認証情報を照合用情報と比較して合致した場合に対応するコマンドを実行するコマンド認証方法。

【請求項2】受信したコマンド中に格納された認証コードから認証情報を抽出する、請求項1に記載のコマンド認証方法。

【請求項3】前記認証コードは非繰り返し数であり、送信側から前記コマンドを送信する際に送信毎に前記認証コードの更新が行われる、請求項2に記載のコマンド認証方法。

【請求項4】前記認証コードは時刻情報または乱数により生成される、請求項3に記載のコマンド認証方法。

【請求項5】前記認証コードは座標アドレスを有する乱数系列表を用いて生成され、送信側から前記コマンドを送信する際に送信毎に座標アドレスを更新することによって前記認証コードの更新が行われる、請求項4に記載のコマンド認証方法。

【請求項6】受信したコマンド中に格納された複数の認証コードから認証情報を抽出する、請求項2に記載のコマンド認証方法。

【請求項7】受信したコマンドの引数が、前記認証コードまたは認証コードから生成された鍵により暗号化されている、請求項2に記載のコマンド認証方法。

【請求項8】受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、前記照合用情報と一致した場合に特定のコマンドを実行する、請求項2に記載のコマンド認証方法。

【請求項9】受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、前記照合用情報と一致した場合にコマンドの引数を追加変更して実行する、請求項2に記載のコマンド認証方法。

【請求項10】受信したコマンド中に格納された認証コードを抽出し、時系列に受信したコマンドの実行を途中で終了した場合、コマンド送受信間の信号を特定状態とする、請求項2に記載のコマンド認証方法。

【請求項11】受信したコマンド中に格納された認証コードを抽出し、この認証コードを特定の記憶領域に保存しておく、請求項8～10のいずれかに記載のコマンド認証方法。

【発明の詳細な説明】

【0001】本発明は、コマンド認証方法、特に、コンピュータなどの外部機器から送信されてくるコマンドを正規のものであるか否かを判別するためのコマンド認証方法に関する。

【発明の属する技術分野】本発明は、コマンド認証方法、特に、コンピュータなどの外部機器から送信されてくるコマンドを正規のものであるか否かを判別するためのコマンド認証方法に関する。

【0002】

【従来の技術】ユーザが任意のデータを書き込むことが可能な記録媒体として、光磁気ディスク(MO)、ディ

ジタルビデオディスク(DVD)、フロッピーディスク(FD)、ミニディスク(MD)などがある。このような記録媒体を駆動するためのドライブは、SCSIインターフェイスなどを介してコンピュータと接続されており、コンピュータから送信されてくるコマンドにより、記録媒体上のデータの書き込み、読み出しが行われる。

【0003】通常、記録媒体は、媒体固有番号を格納している第1階層、特定の情報を格納しておく第2階層、任意の電子化データを格納する第3階層を備えている。第1階層はデータの読み出しは可能であるが書き換えが不可能な領域であり、第2階層はユーザによる読み出し・書き換えが不可能な領域である。また、第3階層は、ユーザが自由に利用できる領域である。

【0004】たとえば、コンピュータプログラムや電子出版物などの電子化データの著作権を保護するために、これら電子化データを所定の暗号鍵で暗号化して第3階層に格納しておくことが考えられる。この場合、第3階層に格納した電子化データの利用権に基づく許諾情報を第2階層に格納しておき、この許諾情報に基づいて正規のユーザが電子化データを復号化して利用することができるようになることが考えられる。このとき、電子化データを格納した記録媒体を配布する際に、復号化するための鍵を許諾情報として第2階層に予め格納しておくことが可能である。また、記録媒体上に格納された電子化データを利用するための利用権をユーザが後に入手した場合に、第2階層にある許諾情報を所定のデータに置き換えて電子化データの復号化を行うように構成してもよい。

【0005】このようにした場合、ユーザはコンピュータ側から特定のコマンドを送信し、第2階層に格納されている所定の情報を読み出したり、書き込んだりする必要がある。この記録媒体の第2階層は、通常はユーザによる書き込み・読み出しが不可能な領域であるため、特定のコマンドが正規のユーザによるものかどうかを判別して実行する必要がある。従来では、ユーザのパスワードを設定しておき、コンピュータ側から特定のコマンドを送出する際に、このコマンドをパスワードに関係付けて送信するように構成している。

【0006】

【発明が解決しようとする課題】上述のようにした場合、パスワードに関するコマンドが独立してコマンドを認証することにより、特定のコマンドが正規のユーザによるものが否かを判別している。しかしながら、第3者によってこのパスワードに関するコマンドを解析されると、特定のコマンドを発行することが可能となり、セキュリティレベルが低下する。特に、コンピュータとドライブとの間のデータバスはモニタすることが可能であり、コンピュータから送出されるコマンドを解析することによってパスワードを入手することは比較的簡単であると考えられる。

【0007】本発明は、第3者から発行されたコマンドが正規のユーザによるコマンドになりすますことを防止し、高いセキュリティを維持するコマンド認証方法を提案する。

【0008】

【課題を解決するための手段】本発明に係るコマンド認証方法は、受信したコマンドから認証情報を抽出し、認証情報を照合用情報と比較して合致した場合に対応するコマンドを実行する。ここで、受信したコマンド中に格納された認証コードから認証情報を抽出するように構成できる。

【0009】また、認証コードは非繰り返し数であり、送信側からコマンドを送信する際に送信毎に認証コードの更新が行われるように構成できる。さらに、認証コードは時刻情報または乱数により生成されたものとすることができる。このとき、認証コードは座標アドレスを有する乱数系列表を用いて生成され、送信側からコマンドを送信する際に送信毎に座標アドレスを更新することによって認証コードの更新が行われるように構成できる。

【0010】また、受信したコマンド中に格納された複数の認証コードから認証情報を抽出する。さらに、受信したコマンドの引数が、認証コードまたは認証コードから生成された鍵により暗号化されたものとすることができる。また、受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、照合用情報と一致した場合に特定のコマンドを実行するように構成できる。

【0011】また、受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、照合用情報と一致した場合にコマンドの引数を追加変更して実行するように構成できる。さらに、受信したコマンド中に格納された認証コードを抽出し、時系列に受信したコマンドの実行を途中で終了した場合、コマンド送受信間の信号を特定状態とすることができる。

【0012】また、受信したコマンド中に格納された認証コードを抽出し、この認証コードを特定の記憶領域に保存しておくように構成できる。

【0013】

【発明の実施の形態】本発明の1実施形態について図を参照して説明する。図1は、装置構成を示す概略ブロック図である。ここでは、パソコンとMOドライブとがSCSIケーブルにより接続されている場合を考える。図1において、ホスト1とMOドライブ2とはデータバス3を介して接続されている。ホスト1は、コマンドの送信側であって、CPU、ROM、RAM、各種インターフェイスなどを備える、いわゆるパーソナルコンピュータである。ホスト1は、コマンド生成部11とコマンド認証コード生成部12とを有している。コマンド生成部11は、MOドライブ2に送信する各種コマンドを生成

する。コマンド認証コード生成部12は、コマンド生成部11で生成されるコマンドが特定のコマンドである場合に、認証情報を付加するために認証コードを生成するものである。

【0014】MOドライブ2は、光磁気ディスク4を駆動するものであって、ホスト1から送信されてくるコマンドに従って、光磁気ディスク4に電子化データを書き込み、また光磁気ディスク4に格納されている電子化データを読み出す。このMOドライブ2も、CPU、ROM、RAM、入出力インターフェイスなどを備えている。MOドライブ2は、コマンド解析部21、コマンド認証コード解析部22、コマンド制御部23を有している。コマンド解析部21は、ホスト1から送信されてくるコマンドをその引数などを含めて解析し、対応するコマンドを発行する。コマンド認証コード解析部22は、送信されてきたコマンドが認証コード付きである場合に、この認証コードを解析して照合用情報と照合し、照合した結果をコマンド解析部21に送信する。コマンド制御部23は、コマンド解析部21から発行されたコマンドに従って、光磁気ディスク4の電子化データを書き込みあるいは読み出しなどの制御を行う。

【0015】ここで、光磁気ディスク4のセキュリティ領域41は、通常ユーザによるアクセスが不可能な領域であるが、コマンド解析部21が特定のコマンドを発行した場合にのみ、このセキュリティ領域41の内容にアクセスできるものとする。ホスト1では、コマンド解析部21が特定のコマンドを発行するために、特定のコマンドを特定の認証コードに関連付けて送出することとなる。

【0016】以下に、具体的な実施形態を説明する。

〔第1実施形態〕第1実施形態では、乱数により認証コードを生成する場合を示す。ホスト1およびMOドライブ2に、図2に示すような2つの共通する乱数系列表51、52を用意する。この乱数系列表51、52の表番号(A)は、それぞれ0、1である。また、乱数系列表51、52は、それぞれ2次元座標のアドレスを備えており、アドレスポインタ(X_i, Y_j)で表されるアドレスにはそれぞれ16進数で表現される1バイトの乱数が格納されている。

【0017】ホスト1側では、図3に示すようなコマンド60をコマンド生成部11で生成する。コマンド60は、オペコード61と、このオペコード61に係る引数62と、オペランドの一部に格納される認証コード63とからなっている。認証コードは、コマンド認証コード生成部12によって生成されるものであり、ここでは、乱数系列表51、52のうちのどちらを選択したかを示す表番号(A)と、選択した乱数系列表の座標を示すアドレスポインタ(x, y)となる。

【0018】このような乱数系列表を用いて認証コード付きのコマンドを送受信する場合には、図4に示すよう

な手順で実行される。まず、ホスト1から初期設定として乱数系列表の開始アドレスを送信する。MOドライブ2では、この開始アドレスを受信して、乱数系列表の初期アドレスの設定を行う。ホスト1から特定のコマンドを発行する場合には、コマンド認証コード生成部12により表番号(A)およびアドレスポインタ(x, y)による認証番号を生成し、さらにこれを通常のコマンドに付加した認証コード付きコマンド60を生成して、MOドライブ2に送信する。MOドライブ2側では、コマンド60のオペランドに格納されている認証コード63を解析して、この認証コード63に基づく乱数系列表の乱数の値を、MOドライブ2側の現在のアドレスポインタによる乱数の値と比較する。この結果が一致した場合には、コマンド解析の結果が正常であった旨の報告をホスト1に送信し、ホスト1では処理を終了する。また、MOドライブ2側では、コマンド60に基づく特定のコマンドを発行し、光磁気ディスク4に対する制御を行う。コマンド解析の結果、乱数の値が一致しない場合には、異常フラグをホスト1に送信する。ホスト1側で異常フラグを受信した場合には、再度認証コード付きのコマンドを生成してMOドライブ2に送信する。MOドライブ2では、認証コード付きコマンドを受信し、上述と同様の動作を繰り返す。

【0019】このように構成した場合、ホスト1が認証コード付きコマンドをMOドライブ2に送信する毎に、認証コードが毎回更新されるので、時系列的なコマンドの送受信をすべてモニタしない限り特定のコマンドを発行させることは困難であり、セキュリティを高く維持することが可能である。2つの乱数系列表を用いて乱数による認証コードを生成したが、1つの乱数系列表だけであってもよく、また、3以上の乱数系列表を用いて認証コードを生成するように構成することも可能である。

〔第2実施形態〕コマンドに付随する引数が特定の鍵によって暗号化されている場合を第2実施形態として示す。

【0020】ホスト1では、図5に示すように、認証コード付きコマンド70を生成する。このコマンド70は、オペコード71と、特定の鍵によって暗号化された第1引数72と、第2引数73と、認証コード74とで構成されている。認証コード74は、たとえば、前述したような乱数系列表を用いて、表番号(A)とアドレスポインタ(x, y)でなるコードとすることができる。第1引数72は、認証コード74で示される乱数系列表の対応する乱数を鍵として暗号化されている。

【0021】このようなコマンド70を受信したMOドライブ2側の動作を図6のフローチャートにより説明する。ステップS1では、認証コード74を解析する。ここでは、乱数系列表を参照して現在のアドレスポインタによる乱数の値が一致しない場合には、異常フラグをホスト1側に送信してエラー処理を行い、値が一致した場

合にはステップS2に移行する。ステップS2では、認証コード74に基づく復号鍵を生成し、これを所定の領域に格納する。

【0022】ステップS3では、オペコード71をデコードする。ステップS4では、認証コード74に基づく復号鍵により第1引数71を復号化する。ステップS5では、コマンドを実行する。この第2実施形態では、第1引数72が暗号化されているため、よりセキュリティを高く維持することができる。

【0023】第2引数73も同様に暗号化して格納することも可能である。

〔第3実施形態〕複数の認証コードを用いる場合について、第3実施形態として説明する。ホスト1では、図7に示すように、認証コード付きコマンド80を生成する。このコマンド80は、オペコード81と、引数82と、第1認証コード83と、第2認証コード84とで構成されている。第1認証コード83と第2認証コード84は、この2つからコマンドの認証を行うための認証コードを生成できるように構成されており、たとえば、2つの認証コードから上述した乱数系列表の次のアドレスポインタを生成するような構成、2つの認証コードのうち一方が暗号化された情報であり他方が復号化する復号鍵であるような構成などが考えられる。

【0024】このようなコマンド80を受信したMOドライブ2側の動作を図8のフローチャートにより説明する。ステップS11では、第1認証コード83および第2認証コード84を読み出す。ステップS12では、読み出した第1認証コード83および第2認証コード84から認証コードを生成する。たとえば、2つの認証コード83、84に基づいて乱数系列表を参照する、一方のコードを他方のコードで復号化するなどして認証コードを生成する。ステップS13では、生成した認証コードを解析して、一致しない場合には、異常フラグをホスト1側に送信してエラー処理を行い、値が一致した場合にはステップS14に移行する。

【0025】ステップS14では、オペコード81をデコードする。ステップS15では、コマンドを実行する。このようにした第3実施形態によれば、第1認証コードおよび第2認証コードから実際の認証コードを生成するためのアルゴリズムを入手することが困難であり、さらに高いセキュリティを維持することが可能となる。

〔第4実施形態〕時系列に受信したコマンド列によって特定のコマンドを発行する場合について、第4実施形態として説明する。

【0026】ホスト1では、図9に示すように、認証コード付きコマンド90を生成する。このコマンド90は、オペコード91と、第1引数92と、第2引数93と、認証コード94とで構成されている。MOドライブ2側では、複数のコマンド列を受信した際に、それぞれの認証コード94を時系列として、特定のパターンであ

るか否かを判別し、特定のパターンであった場合にのみ、特定のコマンドを発行するように構成する。

【0027】たとえば、同一のコマンドAを3個連続して受信した場合に、各コマンドに格納された認証コードが一定のパターンである場合に特定のコマンドを発行するように構成できる。図10に示すように、同一のコマンドAを3個連続して受信した場合、それぞれコマンドに格納された認証コードC1、C2、C3を抽出する。この認証コード列が予めMOドライブ2側で用意したテーブルに合致していれば、特定のコマンドを発行する。

【0028】また、図11に示すように、異なるコマンドA、B、Cを順に受信した場合に、各コマンドに格納された認証コードが一定のパターンである場合に特定のコマンドを発行する構成とすることができる。図11に示すように、異なるコマンドA、B、Cをこの順に受信した場合に、それぞれのコマンドに格納された認証コードC1、C2、C3を抽出する。この認証コード列が予めMOドライブ2側で用意したテーブルに合致していれば、特定のコマンドを発行する。

【0029】このようにした場合には、特定のコマンドを発行するために、複数のコマンドおよび認証コードを必要とし、不正なコマンド制御を防止することができる。複数のコマンドを受信した後、コマンドの実行が途中で終了した場合には、MOドライブ2に格納されている認証コードとキャッシュをクリアするように構成することができる。このことにより、コマンドを受信した際にハッキングが発生しても、認証コードを盗まれることを防止できる。

【0030】また、時系列で受信したコマンドに格納された認証コードを監査情報として順に保存しておく構成とすることができる。この場合には、認証コードの配列またはその個数によりMOドライブ2への不正が行われたか否かを知ることができる。上述した各実施形態において、光磁気ディスク(MO)に代えて、デジタルビ

デオディスク(DVD)、ミニディスク(MD)、フロッピーディスク(FD)、ハードディスク(HD)その他の記録媒体に適用することができる。

【0031】

【発明の効果】本発明によれば、コマンド中の認証情報に基づいて特定のコマンドを実行するように構成しており、認証情報を解析することが困難であり、高いセキュリティを維持することが可能となる。

【図面の簡単な説明】

【図1】装置構成を示す概略ブロック図。

【図2】乱数系列表の説明図。

【図3】第1実施形態に用いられるコマンドの説明図。

【図4】第1実施形態の信号の流れを示す説明図。

【図5】第2実施形態に用いられるコマンドの説明図。

【図6】第2実施形態の制御フローチャート。

【図7】第3実施形態に用いられるコマンドの説明図。

【図8】第3実施形態の制御フローチャート。

【図9】第4実施形態に用いられるコマンドの説明図。

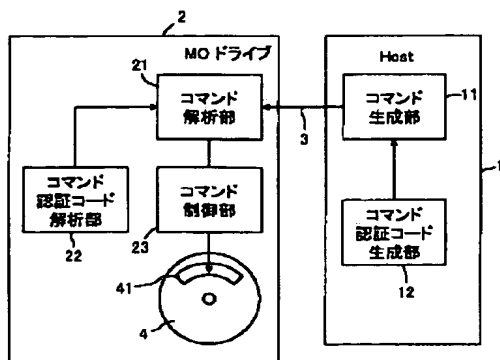
【図10】受信するコマンドの時系列説明図。

【図11】受信するコマンドの時系列説明図。

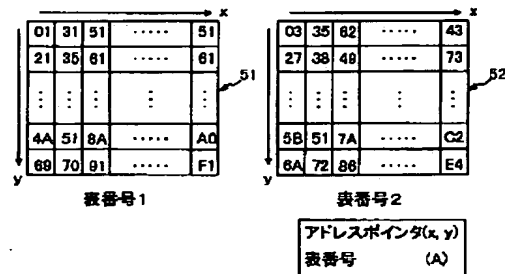
【符号の説明】

- 1 ホスト
- 2 MOドライブ
- 3 データバス
- 4 光磁気ディスク
- 11 コマンド生成部
- 12 コマンド認証コード生成部
- 21 コマンド解析部
- 22 コマンド認証コード解析部
- 23 コマンド制御部
- 4.1 セキュリティ領域
- 5.1 乱数系列表
- 5.2 乱数系列表

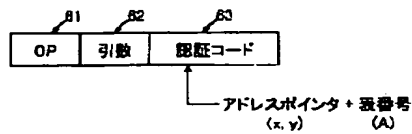
【図1】



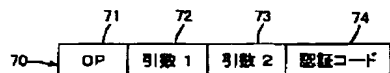
【図2】



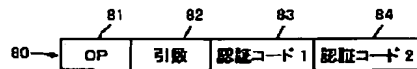
【図3】



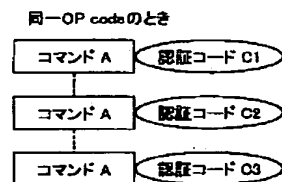
【図5】



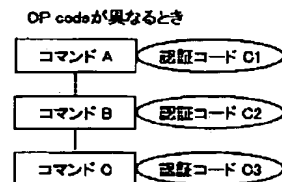
【図7】



【図10】



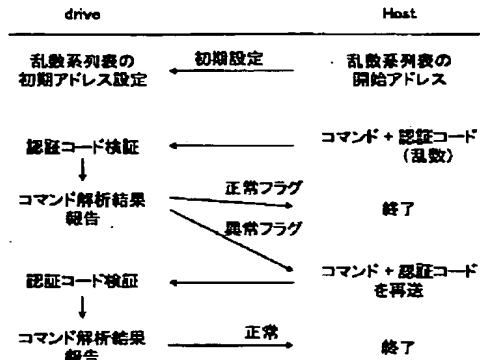
【図11】



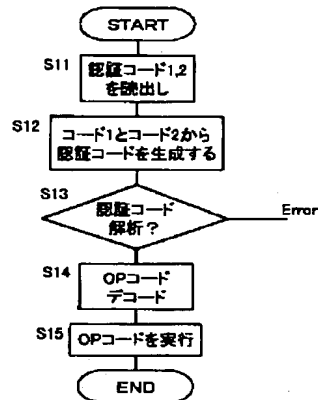
フロントページの続き

(72)発明者 小谷 誠剛
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

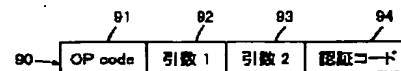
【図4】



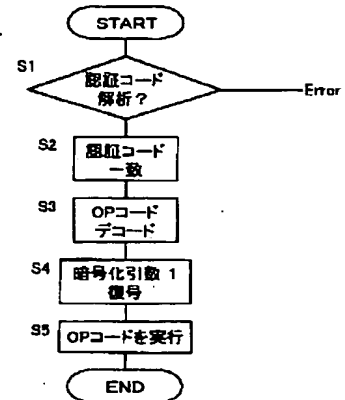
【図8】



【図9】



【図6】



F ターム(参考) 5B017 AA07 BA05 BB02 CA09
5B085 AC03 AE06 AE23 AE29 CC11
CC16
5D044 BC01 BC02 CC04 DE42 DE48
HL02 HL11
5J104 AA07 AA12 GA03 GA05 KA01
NA04 NA32 NA38